Passwort-Checkliste für KMUs (7-Punkte-Sofortprogramm)

1. Richtlinie dokumentieren

- Mindestlänge 12 Zeichen festlegen
- Sonderzeichen vorschreiben (§ 64 BDSG)

2. Passwortmanager einführen

- Bitwarden oder Passbolt installieren
- Master-Passwörter hinterlegen (Chef + Stellvertreter)

3. Zwei-Faktor-Authentifizierung (2FA)

- Für alle Cloud-Dienste aktivieren
- Hardware-Keys für Finanzsysteme

4. Passwortrotation automatisieren

- Kritische Systeme: 60-Tage-Rotation
- Benutzerkonten bei Austritt sofort sperren

5. Schulungen durchführen

- Jährliche verpflichtende Schulungen
- Neue Mitarbeiter in ersten 7 Tagen schulen

6. Notfallzugriffe regeln

- Break-Glass-Accounts einrichten
- Dokumentierte Übergabeprotokolle

7. Audits durchführen

Quartalsweise Passwort-Checks

Penetrationstest alle 12 Monate